CLAIMS

No claims have been amended. This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-19. (cancelled).

20. (previously presented) A method, performed by an intermediary, of leveraging a persistent connection with a client to provide a the client with access to a secured service, the method comprising:

receiving a first request from a client at an intermediary, the first request relating to a request for access to the intermediary;

establishing a persistent connection between the client and the intermediary in response to the first request from the client;

receiving a second request from the client at the intermediary, the second request relating to a request for access to a secured service;

authenticating the intermediary to the secured service responsive to the second request; and

enabling access by the client to the secured service conditioned on whether the intermediary is successfully authenticated to the secured service.

21. (previously presented) The method of claim 20 wherein:

establishing the persistent connection with the client includes authenticating the client to the intermediary based on keystone authentication information provided by the client; and

authenticating the intermediary to the secured service is performed without provision by the client of authentication information duplicative or additional to the keystone information used to establish the persistent connection.

22-23. (cancelled).

24. (previously presented) The method of claim 20 wherein the intermediary is authenticated to the secured service before the client is enabled access to the secured service.

25. (original) The method of claim 20 wherein establishing the persistent connection comprises:

receiving keystone authentication information from the client;

authenticating the client based on the keystone authentication information to provide a keystone authentication associated with the persistent connection; and

establishing the persistent connection with the client based on the keystone authentication.

26. (previously presented) The method of claim 25 wherein the second request from the client for connection to the secured service is received after the persistent connection to the client is established.

27. (previously presented) The method of claim 26 wherein authenticating the intermediary to the secured service includes:

providing a leveraged authentication based on the keystone authentication associated with the persistent connection; and

using the leveraged authentication to establish a connection with the secured service.

28. (original) The method of claim 27 wherein the keystone authentication is used to provide the leveraged authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

29. (cancelled).

30. (previously presented) The method of claim 20 wherein the intermediary comprises a persistent connection service that establishes the persistent connection with the client and a broker service that authenticates the intermediary to the secured service, and authenticating the intermediary includes the broker service receiving from the persistent connection service at a connection request address a communication based on the second request from the client and wherein the connection request address varies systematically with time.

31. (previously presented) The method of claim 20 wherein authenticating the intermediary to the secured service comprises:

determining authorization information based on the second request from the client;

communicating, to the secured service, an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information;

receiving a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service; and

enabling the client to present the authorization information to the secured service to establish the connection with the secured service.

32. (previously presented) The method of claim 20 wherein authenticating the intermediary to the secured service comprises:

communicating, to the secured service, an indication that the client desires to connect to the secured service;

receiving a response from the secured service indicating that the secured service may accept a connection from the client, wherein the response includes authorization information; and

communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

33. (original) The method of claim 32 wherein the authorization information is determined by the secured service.

34. (previously presented) The method of claim 20 wherein:

authenticating the intermediary to the secured service comprises communicating with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

the authorization information comprises constraint information; and

the authorization information may be ineffective to establish a connection with the secured service if one or more connection constraints indicated by the constraint information are not satisfied.

35. (original) The method of claim 34 wherein the connection constraints include a constraint that limits a number of uses for the authorization information to a predetermined threshold number.

36. (original) The method of claim 34 wherein the connection constraints include a constraint that the number of times that the authorization information has been used not exceed a predetermined number of times.

37. (original) The method of claim 34 wherein the connection constraints include a one-time-use password.

38. (original) The method of claim 34 wherein the connection constraints include a constraint that the authorization information be used within a predetermined time window.

39. (original) The method of claim 34 wherein the connection constraints include a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered.

40-54. (cancelled).

55. (previously presented) The method of claim 20 wherein enabling access by the client to the secured service comprises enabling the client to access the secured service independent of the intermediary.

56. (previously presented) The method of claim 55 wherein enabling the client to access the secured service comprises enabling the client to leverage a connection other than the persistent connection established between the client and the intermediary.

57. (previously presented) The method of claim 55 wherein enabling the client to access the secured service comprises providing constrained authentication information to the client.

58. (previously presented) The method of claim 57 wherein the constrained authentication information is provided to the intermediary by the secured service.

59. (previously presented) The method of claim 58 wherein the constrained authentication information is determined by the intermediary and authenticated by the secured service.

60. (previously presented) The method of claim 20 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

61. (previously presented) The method of claim 20 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

62. (previously presented) The method of claim 20 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

63. (previously presented) The method of claim 20 wherein the intermediary is authenticated to the secured service as a consequence of the second request.

64. (previously presented) The method of claim 20 wherein the request for access to the secured service comprises an explicit request for access by the client.

65. (previously presented) The method of claim 20 wherein the request for access to the secured service comprises a client communication received via the secured service.

66. (previously presented) The method of claim 20 wherein the secured service is available for direct authentication by a user without establishing a persistent connection between the user and the intermediary.

67. (previously presented) A method, performed by a client, of leveraging a connection with an intermediary to access a secured service, the method comprising:

receiving a user request for access to a secured service;

submitting, by the client, a request, which is based on the user request for access to a secured service, to an intermediary that is physically distinct of the secured service;

receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request; and

submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary.

68. (previously presented) The method of claim 67 wherein establishing the authenticated connection between the client and the intermediary comprises:

sending, by the client, keystone authentication information to the intermediary; and

receiving, from the intermediary, verification of the keystone authentication information.

69. (previously presented) The method of claim 68 wherein submitting the request to the intermediary for access to the secured service prompts the intermediary to authenticate itself to the secured service without provision by the client of authentication information duplicative or additional to the keystone information.

70. (previously presented) The method of claim 69 wherein the intermediary is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication.

71. (previously presented) The method of claim 67 wherein the constrained authorization information has been issued by the secured service and sent by the secured service to the intermediary.

72. (previously presented) The method of claim 67 wherein the constrained information has been provided by the intermediary and authenticated by the secured service.

73. (previously presented) The method of claim 67 wherein the constrained authorization information comprises one or more of a constraint that the authorization information has been used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

74. (previously presented) The method of claim 67 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

75. (previously presented) The method of claim 67 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

76. (previously presented) The method of claim 67 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file

access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

77. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises an explicit request for access by the client.

78. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises a communication sent by the client to the intermediary via the secured service.

79. (previously presented) The method of claim 67 wherein the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary.

80. (previously presented) The method of claim 67 wherein the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary.

81. (previously presented) A method, performed by a secured service, of allowing a client access based on an authenticated connection between the client and an intermediary, the method comprising:

receiving, at a secured service and from an intermediary, notification of a request by a client to access the secured service;

determining whether a trusted relationship exists between the secured service and the intermediary, responsive to the client request; and

conditioned on the existence of a trusted relationship between the secured service and the intermediary, enabling access by the client to the secured service.

82. (previously presented) The method of claim 81 wherein enabling access by the client comprises issuing constrained authorization information to the intermediary for use by the client to access the secured service.

83. (previously presented) The method of claim 82 wherein enabling access by the client further comprises receiving the constrained authorization information from the client.

84. (previously presented) The method of claim 82 wherein the constrained authorization information comprises one or more of a constraint that the authorization information be used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

85. (previously presented) The method of claim 81 wherein enabling access by the client comprises authenticating constrained authorization information to be provided by the intermediary to the client to access the secured service.

86. (previously presented) The method of claim 85 wherein enabling access by the client further comprises receiving the constrained authorization information from the client.

87. (previously presented) The method of claim 85 wherein the constrained authorization information comprises one or more of a constraint that the authorization information be used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

88. (previously presented) The method of claim 81 wherein enabling access by the client comprises establishing a connection with the client independent of the intermediary.

89. (previously presented) The method of claim 88 wherein the connection between the client and the secured service is established by the client leveraging a connection other than a connection between the client and the intermediary.

90. (previously presented) The method of claim 81 wherein determining whether a trusted relationship exists between the secured service and the intermediary comprises receiving authentication information from the intermediary.

91. (previously presented) The method of claim 90 wherein the intermediary provides the authentication information to the secured service without provision by the client of other authentication information that is duplicative or additional to keystone authentication information provided by the client to the intermediary to establish the authenticated connection between the client and the intermediary.

92. (previously presented) The method of claim 81 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

93. (previously presented) The method of claim 81 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

94. (previously presented) The method of claim 81 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

95. (previously presented). The method of claim 81 wherein the secured service is available for direct authentication by a user without determining whether a trusted relationship exists between the secured service and the intermediary.